

**RECEIVED
CENTRAL FAX CENTER****JAN 17 2006****Yee &
Associates, P.C.**4100 Alpha Road
Suite 1100
Dallas, Texas 75244Main No. (972) 385-8777
Facsimile (972) 385-7766**Facsimile Cover Sheet**

To: Commissioner for Patents for Examiner Thanhnga B. Truong Group Art Unit 2135	Facsimile No.: 571/273-8300
From: Carrie Parker Legal Assistant to Ted Fay	No. of Pages Including Cover Sheet: 45
Message: Enclosed herewith: <ul style="list-style-type: none">• Transmittal Document; and• Appeal Brief.	
Re: Application No. 09/506,225 Attorney Docket No: AUS000101US1	
Date: Tuesday, January 17, 2006	
Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	<i>This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.</i>

**PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY
FAXING A CONFIRMATION TO 972-385-7766.**

RECEIVED
CENTRAL FAX CENTER

JAN 17 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Dutta

Serial No.: 09/506,225

Filed: February 17, 2000

For: Method and Apparatus for
Identifying Universal Resource
Locator Rewriting in a Distributed
Data Processing System

35525

PATENT TRADEMARK OFFICE
CUSTOMER NUMBER§
§
§
§
§
§

Group Art Unit: 2135

Examiner: Truong, Thanhnga B.

Attorney Docket No.: AUS000101US1

Certificate of Transmission Under 37 C.F.R. § 1.8(a)I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (571) 273-8300
on January 17, 2006.

By:

Carrie Parker
Carrie ParkerTRANSMITTAL DOCUMENTCommissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

ENCLOSED HERewith:

- Appeal Brief (37 C.F.R. 41.37)

A fee of \$500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Theodore D. Fay IIITheodore D. Fay III
Registration No. 48,504

Duke W. Yee

Registration No. 34,285

YEE & ASSOCIATES, P.C.

P.O. Box 802333

Dallas, Texas 75380

(972) 385-8777

ATTORNEYS FOR APPLICANT

RECEIVED
CENTRAL FAX CENTER

JAN 17 2006

Docket No. AUS000101US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Dutta

Serial No. 09/506,225

Filed: February 17, 2000

For: Method and Apparatus for
Identifying Universal Resource
Locator Rewriting in a Distributed
Data Processing System§
§
§
§
§
§
§

Group Art Unit: 2135

Examiner: Truong, Thanhnga B.

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450Certificate of Transmission Under 37 C.F.R. § 1.8(a)I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (571) 273-8300
on January 17, 2006.

By:

Carris Parker
Carris Parker

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on November 14, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this
brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

01/18/2006 EAYALEW1 00000023 090447 09506225

01.FC:1402 500.00 DA

(Appeal Brief Page 1 of 43)
Dutta - 09/506,225

REAL PARTY IN INTEREST

The real party in interest in this appeal is International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-39

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-39
4. Claims allowed: None
5. Claims rejected: 1-39
6. Claims objected to: None

C. CLAIMS ON APPEAL

The claims on appeal are: 1-39

STATUS OF AMENDMENTS

No amendments were filed after the final office action of September 22, 2005.

**RECEIVED
CENTRAL FAX CENTER****JAN 17 2006****SUMMARY OF CLAIMED SUBJECT MATTER****A. CLAIM 1 - INDEPENDENT**

Claim 1 is directed to a method in a data processing system for detecting monitoring of access to content (Page 6, lines 3-5; Page 9, lines 3-5; Page 13, lines 27-30; Page 20, lines 10-13). The method includes requesting the content from a source using a set of identifiers (Page 6, lines 5-6; Page 14, lines 1-3; Page 14, line 20; Page 16, lines 19-26; Page 20, lines 16-19; Page 24, lines 7-8; Figure 4, reference numbers 400-408; Figure 5, reference number 500; Figure 7, reference number 700); receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content (Page 16, lines 19-26; Page 20, line 28; Figure 4, reference numbers 400-408; Figure 7, reference number 704); sending identifiers to a validation service, wherein the identifiers include the set of identifiers used to request the received content and each returned identifier representing the location of the content at the source (Page 6, lines 6-9; Page 14, lines 3-7; Page 15, lines 4-8; Page 16, line 29-page 17, line 13; Page 20, lines 19-22; Page 24, lines 8-9; Figure 4, reference numbers 400-410; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference numbers 800-804); and responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, selectively preventing receipt of additional content from the source (Page 6, lines 14-17; Page 14, lines 9-15; Page 16, lines 5-8; page 17, lines 19-25; Page 17, lines 28-30; Page 19, lines 18-21; Figure 4, reference numbers 400-404 and 410-412; Figure 7, reference numbers 706-716).

B. CLAIM 8 - INDEPENDENT

Claim 8 is directed to method in a data processing system for detecting monitoring of access to content (page 6, lines 3-5; page 9, lines 3-5; page 13, lines 27-30; page 20, lines 10-13; page 22, lines 21-24; Figure 7, reference numerals 700-712). The method includes receiving a request from a requestor to determine whether a source of the content is monitoring access by the requestor, wherein the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to

(Appeal Brief Page 6 of 43)
Dutta - 09/506,225

the first number of identifiers (Page 14, lines 3-7; Page 15, lines 4-13; Page 16, line 29-page 17, line 6; Page 20, lines 19-22; Page 22, lines 1-3; Figure 4, reference numbers 400-404 and 410-412; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference number 800); sending a new request to the source using an identifier from the first number of identifiers in the set of identifiers (page 15, lines 14-16; page 15, lines 19-21; page 17, lines 7-9; page 22, line 4, Figure 4, reference numbers 402-408 and 410-412; Figure 8, reference numbers 802-804); receiving a first response from the source, wherein the response includes a return identifier (page 15, lines 16-19; page 17, lines 9-20; page 22, lines 4-7; Figure 4, reference numbers 402-408 and 410-412; Figure 5, reference number 506; Figure 8, reference number 806-807); comparing the set of identifiers to the return identifier (page 14, lines 7-11; page 15, lines 21-22; page 17, lines 10-22; page 22, lines 7-12; Figure 5, reference numbers 504-508; Figure 8, reference numbers 810-816); and generating a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers (Page 14, lines 11-13; Page 16, lines 2-4; Page 17, lines 22-26; Page 22, lines 9-18; Figure 7, reference number 712; Figure 8, reference number 818).

C. CLAIM 16 - INDEPENDENT

Claim 16 is directed to a browser program for use in a data processing system (Page 9, lines 3-5; Page 18, lines 6-9; Page 26, lines 24-25; Figure 4, reference number 404; Figure 6, reference number 600). The browser includes a communications interface, wherein the communications interface receives content from a network (Page 18, lines 24-29; Page 26, lines 25-27; Figure 6, reference number 610); a graphical user interface used to display the content (Page 18, lines 9-17; Page 26, line 28; Figure 6, reference number 620); a language interpretation unit, wherein the language interpretation unit processes content received by the communications interface for display on the graphical user interface (Page 18, line 30-page 19, line 7; Page 26, line 29-page 27, line 1; Figure 6, reference numbers 612-616); and a detection unit (Page 19, lines 8-21; Figure 6, reference number 618), wherein the detection unit requests the content from a source using a set of identifiers (Page 15, lines 14-16; Page 19, lines 10-14; Page 22, lines 2-5, Figure 4, reference numbers 402-408 and 410-412; Figure 8, reference numbers 802-804); receives the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the contents at the source (Page 15, lines

16-19; Page 17, lines 9-20; Page 22, lines 4-7; Figure 4, reference numbers 402-408 and 410-412; Figure 5, reference number 506; Figure 8, reference number 806-807); sends identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the received content (Page 6, lines 6-9; Page 14, lines 3-7; Page 15, lines 4-8; Page 16, line 29-page 17, line 13; Page 20, lines 19-22; Page 24, lines 8-9; Figure 4, reference numbers 400-410; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference numbers 800-804); and selectively prevents receipt of additional content from the source in response to receiving a response from the validation service indicating the monitoring of user requests to access to received content is occurring (Page 6, lines 14-17; page 14, lines 9-15; Page 16, lines 5-8; page 17, lines 19-25; Page 17, lines 28-30; Page 19, lines 18-21; Figure 4, reference numbers 400-404 and 410-412; Figure 7, reference numbers 706-716).

D. CLAIM 19 - INDEPENDENT

Claim 19 is directed to a data processing system (Page 9, lines 3-5). The data processing system includes a bus (Page 10, lines 18-28, Page 11, lines 1-10; Page 11, line 26-page 12, line 19; Page 27, line 18; Figure 2, reference numbers 206, 212, 216, 226, and 228; Figure 3, reference number 306); a communications interface connected to the bus, wherein the communications interface is configured for connection to a network (Page 10, line 24-page 11, line 2; Page 27, lines 19-21; Figure 2, reference numbers 212-218); a processing unit connected to the bus, wherein the processing unit executes instructions (Page 10, lines 14-18; Page 11, line 31-page 12, line 3; Page 27, lines 22-23; Figure 2, reference numbers 202-206; Figure 3, reference numbers 302, 306, and 308); and a memory connected to the bus (Page 10, lines 18-23; Page 12, lines 2-3; Page 27, lines 24-30; Figure 2, reference numbers 202-206; Figure 3, reference numbers 304-308), wherein the memory includes instructions used to request the content from a source using a set of identifiers; receive the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the received contents at the source (Page 6, lines 5-6; Page 14, lines 1-3; Page 14, line 20; Page 16, lines 19-26; Page 20, lines 16-19; Page 24, lines 7-8; Figure 4, reference numbers 400-408; Figure 5, reference number 500; Figure 7, reference number 700); send identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each

returned identifier representing the location of the received content (Page 6, lines 6-9; Page 14, lines 3-7; Page 15, lines 4-8; Page 16, line 29-page 17, line 13; Page 20, lines 19-22; Page 24, lines 8-9; Figure 4, reference numbers 400-410; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference numbers 800-804); and selectively prevent receipt of additional content from the source in response to receiving a response from the validation service indicating monitoring of user requests to access to the received content is occurring (page 6, lines 14-17; page 14, lines 9-15; page 16, lines 5-8; page 17, lines 19-25; page 17, lines 28-30; page 19, lines 18-21; Figure 4, reference numbers 400-404 and 410-412; Figure 7, reference numbers 706-716).

E. CLAIM 21 - INDEPENDENT

Claim 21 is directed to a data processing system (Page 9, lines 3-5). The data processing system includes a bus (Page 10, lines 18-28, Page 11, lines 1-10; Page 11, line 26-page 12, line 19; Page 28, line 6; Figure 2, reference numbers 206, 212, 216, 226, and 228; Figure 3, reference number 306); a communications interface connected to the bus, wherein the communications interface is configured for connection to a network (Page 10, line 24-page 11, line 2; Page 28, lines 7-9; Figure 2, reference numbers 212-218); a processing unit connected to the bus, wherein the processing unit executes instructions (Page 10, lines 14-18; Page 11, line 31-page 12, line 3; Page 28, lines 10-11; Figure 2, reference numbers 202-206; Figure 3, reference numbers 302, 306, and 308); and a memory connected to the bus (Page 10, lines 18-23; Page 12, lines 2-3; Page 28, line 12; Figure 2, reference numbers 202-206; Figure 3, reference numbers 304-308), wherein the memory includes instructions used to receive a request from a requestor to determine whether a source of the content is monitoring access by the requestor in which the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to the first number of identifiers (page 14, lines 3-7; page 15, lines 4-13; page 16, line 29-page 17, line 6; page 20, lines 19-22; page 22, lines 1-3; Figure 4, reference numbers 400-404 and 410-412; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference number 800); send a new request to the source using an identifier from the first number of identifiers in the set of identifiers (page 15, lines 14-16; page 15, lines 19-21; page 17, lines 7-9; page 22, line 4, Figure 4, reference numbers 402-408 and 410-412; Figure 8,

reference numbers 802-804), receive a first response from the source in which the response includes a return identifier (page 15, lines 16-19; page 17, lines 9-20; page 22, lines 4-7; Figure 4, reference numbers 402-408 and 410-412; Figure 5, reference number 506; Figure 8, reference number 806-807), compare the set of identifiers to the return identifier (page 14, lines 7-11; page 15, lines 21-22; page 17, lines 10-22; page 22, lines 7-12; Figure 5, reference numbers 504-508; Figure 8, reference numbers 810-816), and generate a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers (page 14, lines 11-13; page 16, lines 2-4; page 17, lines 22-26; page 22, lines 9-18; Figure 7, reference number 712; Figure 8, reference number 818).

F. CLAIM 22 - INDEPENDENT

Claim 22 is directed to a data processing system for detecting monitoring of access to content (Page 6, lines 3-5; Page 9, lines 3-5; Page 13, lines 27-30; Page 20, lines 10-13). The data processing system includes requesting means for requesting the content from a source using a set of identifiers (Page 6, lines 5-6; Page 14, lines 1-3; Page 14, line 20; Page 16, lines 19-26; Page 20, lines 16-19; Page 24, lines 7-8; Figure 4, reference numbers 400, 402, 404, and 408; Figure 5, reference number 500; Figure 7, reference number 700); receiving means for receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content at the source (Page 16, lines 19-26; Page 20, line 28; Figure 4, reference numbers 400-408; Figure 7, reference number 704); sending means for sending identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the received content (Page 6, lines 6-9; Page 14, lines 3-7; Page 15, lines 4-8; Page 16, line 29-page 17, line 13; Page 20, lines 19-22; Page 24, lines 8-9; Figure 4, reference numbers 400-410; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference numbers 800-804); and preventing means responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, for selectively preventing receipt of additional content from the source (Page 6, lines 14-17; Page 14, lines 9-15; Page 16, lines 5-8; page 17, lines 19-25; Page 17, lines 28-30; Page 19, lines 18-21; Figure 4, reference numbers 400-404 and 410-412; Figure 7,

reference numbers 706-716).

G. CLAIM 26 - DEPENDENT

Claim 26 is directed to the data processing system of claim 22, wherein the preventing means comprises presenting means for presenting an indication of monitoring of user requests to access the content is occurring by the source (Page 18, lines 9-12; Page 19, lines 18-25 ;Page 21, lines 9-13 and lines 15-17; page 22, lines 11-13; Figure 6, reference numbers 602 and 620); and means, responsive to receiving user input indicating that receipt of the additional content from the source should be prevented, for preventing receipt of additional content from the source.

H. CLAIM 27 - DEPENDENT

Claim 27 is directed to the data processing system of claim 26, wherein the preventing means comprises including means for including an identification of the source in a service used to prevent receipt of content from identified sources (Page 14, lines 13-15; Page 16, lines 5-10; Page 17, line 28-page 18, line 5; Page 19, lines 17-21; Page 21, lines 15-16; Page 22, lines 11-12; Figure 4, reference numbers 400, 402, and 404; Figure 6, reference number 618)

I. CLAIM 29 - INDEPENDENT

Claim 29 is directed to a data processing system for detecting monitoring of access to content (Page 6, lines 3-5; Page 9, lines 3-5; Page 13, lines 27-30; Page 20, lines 10-13). The data processing system includes first receiving means for receiving a request from a requestor to determine whether a source of the content is monitoring access by the requestor, wherein the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to the first number of identifiers (page 14, lines 3-7; page 15, lines 4-13; page 16, line 29-page 17, line 6; page 20, lines 19-22; page 22, lines 1-3; Figure 4, reference numbers 400-404 and 410-412; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference number 800); sending means for sending a new request to the source using an identifier from the first number of identifiers in the set of identifiers (page 15, lines 14-16; page 15, lines 19-21; page 17, lines 7-9;

page 22, line 4, Figure 4, reference numbers 402-408 and 410-412; Figure 8, reference numbers 802-804); second receiving means for receiving a first response from the source, wherein the response includes a return identifier (page 15, lines 16-19; page 17, lines 9-20; page 22, lines 4-7; Figure 4, reference numbers 402-408 and 410-412; Figure 5, reference number 506; Figure 8, reference number 806-807); comparing means for comparing the set of identifiers to the return identifier (page 14, lines 7-11; page 15, lines 21-22; page 17, lines 10-22; page 22, lines 7-12; Figure 5, reference numbers 504-508; Figure 8, reference numbers 810-816); and generating means for generating a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers (Page 14, lines 11-13; Page 16, lines 2-4; Page 17, lines 22-26; Page 22, lines 9-18; Figure 7, reference number 712; Figure 8, reference number 818).

J. CLAIM 35 - DEPENDENT

Claim 35 is directed to the data processing system of claim 29, wherein the generating means comprises: placing means for placing an identification of the source in the response. (Specification, p. 17, ll. 25-27).

K. CLAIM 37 - INDEPENDENT

Claim 37 is directed to a computer program product in a computer readable medium for detecting monitoring of access to content (Page 6, lines 3-5; Page 9, lines 3-5; Page 13, lines 27-30; Page 20, lines 10-13; and Page 22, line 22-page 23, line 10). The computer program product includes first instructions for requesting the content from a source using a set of identifiers (Page 6, lines 5-6; Page 14, lines 1-3; Page 14, line 20; Page 16, lines 19-26; Page 20, lines 16-19; Page 24, lines 7-8; Figure 4, reference numbers 400-408; Figure 5, reference number 500; Figure 7, reference number 700); second instructions for receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content at the source (Page 16, lines 19-26; Page 20, line 28; Figure 4, reference numbers 400-408; Figure 7, reference number 704); third instructions for sending identifiers used to reach the received content to a validation service, wherein the identifiers include each identifier used to request the received content and each returned identifier representing the location of the received content (Page 6, lines 6-9; Page 14, lines 3-7; Page 15, lines

4-8; Page 16, line 29-page 17, line 13; Page 20, lines 19-22; Page 24, lines 8-9; Figure 4, reference numbers 400-410; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference numbers 800-804); and fourth instructions, responsive to a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, for selectively preventing receipt of additional content from the source (Page 6, lines 14-17; Page 14, lines 9-15; Page 16, lines 5-8; page 17, lines 19-25; Page 17, lines 28-30; Page 19, lines 18-21; Figure 4, reference numbers 400-404 and 410-412; Figure 7, reference numbers 706-716).

L. CLAIM 38 - INDEPENDENT

Claim 38 is directed to a computer program product in a computer readable medium for detecting monitoring of access to content (page 6, lines 3-5; page 9, lines 3-5; page 13, lines 27-30; page 20, lines 10-13; page 22, lines 21-24; Page 22, line 22-page 23, line 10; and Figure 7, reference numerals 700-712). The computer program product includes first instructions for receiving a request from a requestor to determine whether a source of the content is monitoring access by the requestor, wherein the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to the first number of identifiers (Page 14, lines 3-7; Page 15, lines 4-13; Page 16, line 29-page 17, line 6; Page 20, lines 19-22; Page 22, lines 1-3; Figure 4, reference numbers 400-404 and 410-412; Figure 5, reference number 504; Figure 7, reference number 702; Figure 8, reference number 800); second instructions for sending a new request to the source using an identifier from the first number of identifiers in the set of identifiers (page 15, lines 14-16; page 15, lines 19-21; page 17, lines 7-9; page 22, line 4, Figure 4, reference numbers 402-408 and 410-412; Figure 8, reference numbers 802-804); third instructions for receiving a first response from the source, wherein the response includes a return identifier (page 15, lines 16-19; page 17, lines 9-20; page 22, lines 4-7; Figure 4, reference numbers 402-408 and 410-412; Figure 5, reference number 506; Figure 8, reference number 806-807); fourth instructions for comparing the set of identifiers to the return identifier (page 14, lines 7-11; page 15, lines 21-22; page 17, lines 10-22; page 22, lines 7-12; Figure 5, reference numbers 504-508; Figure 8, reference numbers 810-816); and fifth instructions for generating a second response indicating the monitoring of access by the requestor

for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers (Page 14, lines 11-13; Page 16, lines 2-4; Page 17, lines 22-26; Page 22, lines 9-18; Figure 7, reference number 712; Figure 8, reference number 818).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL**A. GROUND OF REJECTION 1 (Claims 1-39)**

Claims 1-39 stand rejected under 35 U.S.C. § 103(a) as obvious over *Ogden et al.*, Method and System for Providing a Presentation on a Network, U.S. Patent 6,161,137 (Dec. 12, 2000) (hereinafter "Ogden").

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-39)

A.1 Claims 1-4 and 7-39

Claims 1-4 and 7-39 stand rejected under 35 U.S.C. § 103(a) as obvious over *Ogdon et al.*, Method and System for Providing a Presentation on a Network, U.S. Patent 6,161,137 (Dec. 12, 2000). Claim 1 is a representative claim of this group of claims:

1. A method in a data processing system for detecting monitoring of access to content, the method comprising the data processing system implemented steps of:
 - requesting the content from a source using a set of identifiers;
 - receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content;
 - sending identifiers to a validation service, wherein the set of identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the content at the source; and
 - responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, selectively preventing receipt of additional content from the source.

The examiner failed to state a *prima facie* case of obviousness against claim 1 because (i) features that the examiner states as being present in *Ogdon* are not taught or suggested in *Ogdon*, (ii) the examiner has failed to state a proper motivation to modify the reference, (iii) *Ogdon* is non-analogous art, (iv) *Ogdon* addresses a different problem than that addressed by claim 1, (v) claim 1 solves a problem unrecognized by *Ogdon*, and (vi) because the proposed modification would result in an unworkable method.

A.1.1 The Examiner Failed to State a Prima Facie Obviousness Rejection Against Claim 1 Because Features that the Examiner States as Being Present in Ogdon Are Not Taught or Suggested in Ogdon

The examiner failed to state a *prima facie* obviousness rejection because the features that the examiner states as being present in *Ogdon* are not found or suggested in *Ogdon*. In particular, *Ogdon* does not teach or suggest the claimed features of (a) receiving content and at least one returned identifier, (b) sending the set of identifiers used to request the received content and each

and therefore have been provided with validation information (e.g. a presentation performance identifier and/or password) for validating each client as an audience member for the presentation. Subsequently, in step 420, a determination is made by the pre-show control system 136 as to whether each candidate presentation audience member is connected to the pre-show control system by the communications network 70 or by the telephony network 74. If it is determined that a candidate presentation client is connected by the communications network 70, then step 424 is performed, wherein the candidate client logs onto the pre-show control 136 with a previously provided login. Note that this login may include a presentation performance identifier for the presentation and a password for identifying the candidate client as being registered for the presentation performance. Further note that in one embodiment, this step is performed by the lobby system 144. Subsequently, in step 428, a determination is made by the pre-show control system 136 (or the lobby system 144) as to whether the entered login is valid. If the login is determined to be invalid, then step 432 is performed wherein the connection with the pre-show control system 136 is terminated. Note however, it is within the scope of the present invention that various retries can be provided as one skilled in the art will understand. Alternatively, if the candidate client's login is determined to be valid, then step 436 is performed wherein the pre-show control (determines whether the client's client node 56 is configured appropriately for the presentation performance). In particular, the pre-show control system 136 determines whether the client presentation software 88 is operable on the client's client node 56. Further, the pre-show control system 136 may also determine whether the client's client node 56 has the appropriate network 70 addresses (e.g. URLs) of the content webserver 96 available for supplying presentation segments to the client node.

Ogdon, col. 18, l. 57 through col. 19, l. 29.

In summary, a client first registers to view a presentation performance and is provided a presentation identifier. Next, on the date and time the presentation performance is given, the client supplies the presentation identifier, and the validation server determines whether the presentation identifier is valid or not. If the validation server determines that the client's presentation identifier is valid, the client is then allowed to access presentation content. But, if the identifier is not valid, the connection is terminated and the client is not allowed to access *any* presentation content. Thus, the validation server is provided and asked to validate a presentation identifier *before* the client is allowed access to any content, and if the identifier is not valid, the termination of the connection prevents the client from accessing any presentation content.

In contrast, in claim 1, a user requests access to content using a set of identifiers and receives

content and returned identifiers. Claim 1 also recites that the validation service is then provided (i) the identifiers used to receive the content and (ii) the returned identifiers to determine whether user requests to access content is being monitored. If the validation service determines monitoring of user requests to access content is occurring, then the user is selectively prevented from receiving additional content from that source. Thus, in claim 1, the validation service is provided the set of identifiers used to access the content and the returned identifiers *after* the user receives content.

Because *Ogdon's* validation server validates whether a client is authorized to access a presentation, only the presentation identifier is provided to the validation server for validation. *Ogdon* does not provide the returned identifiers to the validation server. In contrast, in claim 1, the validation service is provided (1) the identifiers used to access the content and (2) the returned identifiers.

Thus, *Ogdon's* validation server validates the presentation identifier *before* a client can access any presentation content to prevent unauthorized clients from accessing presentations. In contrast, the present invention allows a user to receive content and returned identifiers, and *afterwards* validates whether monitoring of user requests to access content are occurring. In claim 1, the validation service validates different parameters, occurs in a different context (after rather than before receiving content), and serves a different purpose. Nothing in *Ogdon* suggests otherwise. Thus, the reference does not teach or suggest all the features of claim 1 as asserted by the examiner.

Regarding the feature of selectively preventing receipt of additional content from the source, the examiner acknowledges that *Ogdon* does not show this feature. Office Action of April 19, 2005, p.

4. The examiner goes on to assert that *Ogdon* implies this feature, citing the following portion of *Ogdon*:

Content manager 104 distributes presentation content (e.g., presentation segments) to the content web servers 96 and verifies that the content is capable of being presented to audience members immediately before a presentation time. Note that the verification process makes sure that all the links in the presentation or show can be resolved appropriately. Finally, at the end of a presentation performance, the content manager 104 may remove the presentation content from one or more of the content web servers 96.

Ogdon, col. 9, ll. 44-53.

However, contrary to the examiner's assertions, the cited portion of *Ogdon* does not teach or suggest selectively preventing receipt of *additional* content from the source. *Ogdon* teaches

removing presentation content at the end of a presentation after the client has accessed the content. *Ogdon* also teaches preventing unauthorized clients from accessing presentation content. *Ogdon* does not teach a user accessing and receiving content, detecting whether the user's requests to access content are being monitored, and then preventing receipt of additional content if the user's requests are being monitored.

In *Ogdon*, clients with valid presentation identifiers can access content while clients with invalid presentation identifiers do not get access to any content. Thus, in *Ogdon*, access to content is determined by the validity of the presentation identifier. In contrast, in claim 1, after the user initially receives content and a set of returned identifiers, if the validation service detects monitoring of user requests to access content is occurring, then the user is selectively prevented from receiving *additional* content. Thus, in the present invention, access to content is not determined by the validity of the presentation identifier. Unlike *Ogdon*, in claim 1 access to content is determined by whether or not the content provider is monitoring user requests to access content. Thus, the proposed interpretations of the cited reference are incorrect. Accordingly, the examiner has failed to state a *prima facie* obviousness rejection of claim 1.

In summary, *Ogdon* does not teach or suggest the claimed features of receiving content and at least one returned identifier, sending the identifiers used to request the content and each returned identifier to a validation service, or selectively preventing receipt of additional content from the source responsive to the validation service indicating monitoring of user requests to access content is occurring. Therefore, the examiner has failed to state a *prima facie* obviousness rejection against claim 1.

Nevertheless, in the response to arguments, the examiner states that:

Examiner totally disagrees with applicant's remark and still maintains that:

Ogdon does teach the claimed subject matter. The present invention is a network presentation distribution system for providing a presentation, via one or more communication networks, to a plurality of presentation members simultaneously. That is, the present invention distributes a presentation synchronously to presentation members via the one or more communication networks, wherein a communication network is defined as both the physical components and the communication protocol(s) utilized on the network components and wherein the term, "presentation members" (also denoted "users"), includes both audience members (also denoted "clients") and presentation leaders. Moreover, the present invention provides interactive and/or real-time presentations to presentation members

(Appeal Brief Page 20 of 43)
Dutta - 09/506,225

that are geographically scattered when each such member has access to one or more commonly available communication networks such as the Internet and a conventional telephony network for telephone-to-telephone voice communication. For example, the present invention may communicate the video portion of a presentation to a user site via the Internet (more generally, via any TCP/IP network) while a corresponding audio portion may be communicated to the user site via a conventional telephony network and a conventional telephone at the user site. However, other embodiments are also within the scope of the present invention. For example, both the video and audio portions of the presentation may be provided solely by a TCP/IP network such as the Internet, assuming that there is sufficient communication bandwidth to synchronize presentation transmissions to the presentation members (column 1, lines 54-67 through column 2, lines 1-15 of Ogdon).

Office Action of September 22, 2005 (pp. 11-12).

However, the examiner has failed to address any of the points discussed above. Instead, the examiner appears to have merely repeated portions of Ogdon that are irrelevant to the claimed invention. The fact remains, as explained above, that Ogdon does not teach or suggest the claimed features of (a) receiving content and at least one returned identifier, (b) sending the set of identifiers used to request the received content and each returned identifier to a validation service, or (c) responsive to the validation service indicating monitoring of user requests to access content is occurring, selectively preventing receipt of additional content from the source. The text that the examiner repeats does not teach or suggest these features, and the examiner fails to address how Ogdon could possibly teach these features. Certainly, the examiner utterly fails to rebut any of the facts shown above. Given that Ogdon does not teach or suggest all of the features of claim 1 as asserted by the examiner, and further given that no teaching or suggestion exists to further modify Ogdon to achieve the claimed invention, the examiner continues to fail to state a *prima facie* obviousness rejection against claim 1.

A.1.ii The Examiner Failed To State a Prima Facie Obviousness Rejection Against Claim 1 Because the Examiner Has Failed To State a Proper Motivation To Modify the Reference

The examiner has failed to state a *prima facie* obviousness rejection because the examiner has failed to state a proper motivation to modify Ogdon. The examiner states that an "ordinary skilled person would have been motivated to "... prevent unauthorized members from using/accessing the

(Appeal Brief Page 21 of 43)
Dutta - 09/306,225

content". Office Action of April 19, 2005, p. 4. However, this statement does not state any motivation to modify the reference to detect monitoring of user's requests to access content. The cited reference discusses monitoring client requests to access presentation content but there is no motivation in the reference to detect when monitoring of requests occurs. Because the examiner must state a proper motivation to modify the reference, the examiner has failed to state a *prima facie* obviousness rejection.

Similarly, the examiner has provided no support for the proposition that allowing registered clients access to a presentation on a network using a presentation identifier and detecting monitoring of user requests to access content are in any way equivalent. Thus, the examiner's statement is logically insufficient to establish that one feature may be substituted for another or that a motivation exists to modify Ogden. Accordingly, again, the examiner has failed to state a *prima facie* obviousness rejection.

The examiner has also failed to state any motivation as to why detecting when a content site is monitoring user requests to access content would be obvious in view of *Ogdon*. *Ogdon* makes a presentation available to clients on a network, so *Ogdon* teaches validating a presentation identifier to determine whether a client is authorized to access the presentation. However, there is no motive to validate whether monitoring of user access to content is occurring because in *Ogdon*, once the user has access to the content, validation has already been performed. The examiner has thus failed to state a proper motivation to modify *Ogdon* to achieve these claimed features. The examiner has accordingly failed to state a *prima facie* obviousness rejection.

In addition, the examiner's statement does not serve as a proper motivation to modify *Ogdon* because the statement makes no sense vis-à-vis *Ogdon* and claim 1. Claim 1 provides for selectively preventing receipt of content responsive to a response from a validation service indicating that monitoring of user requests to access the received content is occurring. The examiner's statement refers to selectively blocking unauthorized users, while the claimed method requires preventing receipt of content if monitoring is occurring. Thus, if the examiner's statement were used to modify *Ogdon*, then all users would be prevented from receiving content as soon as the content provider started monitoring. This result would be contrary to *Ogdon*'s purpose of making a presentation available to users, and so the examiner's statement cannot be construed as motivation to modify *Ogdon*. Accordingly, the examiner has failed to state a *prima facie* case of obviousness.

Nevertheless, in response to arguments, the examiner states that:

In response to applicant's argument that there is no motivation to modify the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. [References Omitted.] In this case, the teaching of Ogdon is sufficient.

Office Action of September 9, 2005, p. 12.

Again, the examiner utterly fails to address any of the facts raised above and in the previous response to office action. As shown above, Ogdon does not teach or suggest everything that the examiner asserts that Ogdon teaches. Thus, the teachings of Ogdon are, by themselves, inherently insufficient to motivate one of ordinary skill to modify Ogdon to achieve the invention of claim 1. The examiner's statement does not negate the fact that the examiner's previously stated motivation to modify Ogdon makes no sense vis-à-vis claim 1. The examiner's statement does not negate the fact that there is no motive to validate whether monitoring of user access to content is occurring because, in *Ogdon*, once the user has access to the content, validation has already been performed. Thus, the examiner continues to fail to provide a motivation to modify Ogdon. Accordingly, the examiner continues to fail to state a prima facie obviousness rejection against claim 1.

A.1.iii The Examiner Failed To State a Prima Facie Obviousness Rejection Against Claim 1 Because Ogdon Is Non-Analogous Art

The examiner has failed to state a *prima facie* obviousness rejection against claim 1 because *Ogdon* is non-analogous art and therefore the examiner may not use *Ogdon* as a reference. "In order to rely on a reference as a basis for rejection of the applicant's invention, the reference must either be in the field of the applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." *In re Oetiker*, 977 F.2d 1443, 1447 (Fed. Cir. 1992).

Ogdon is in the field of providing a presentation on a network. *Ogdon*, col. 1, ll. 1-2. On the other hand, the claimed invention is in the field of identifying rewriting of universal resource locators in content requested by a user. Specification, p. 1, ll. 13-14. These two fields are different from each other. Because the fields are distinct, *Ogdon* fails the first test of *Oetiker*.

(Appeal Brief Page 23 of 43)
Dutta - 09/306,225

In addition, *Ogdon* is not reasonably pertinent to the particular problem solved by the present invention. *Ogdon* pertains to the problem of delivering a presentation to users with differing network characteristics. *Ogdon*, col. 1, ll. 9-15. In contrast, the invention of claim 1 pertains to the problem of ensuring a user's privacy when a website is monitoring user behavior. Specification, p. 3, ll. 22-25; claim 1. These two problems have nothing to do with each other and so *Ogdon* is not reasonably pertinent to the problem to be solved. Hence, *Ogdon* also fails the second test of *Oetiker*.

Moreover, In *In re Oetiker*, the Court held "it has not been shown that a person of ordinary skill, seeking to solve a problem of fastening a hose clamp, would reasonably be expected or motivated to look to fasteners for garments." *Id.* The Court found that even though fasteners for hose clamps are similar to fasteners for garments, the latter is non-analogous art to the former. *Id.* In the case at hand, *Ogdon* is completely dissimilar to the invention of claim 1, for the reasons presented above. Given that the claimed invention is much more dissimilar to *Ogdon* than fasteners for garments are dissimilar to fasteners for hose clamps; *Ogdon* is non-analogous art to claim 1 under the standards of *In re Oetiker*.

Because *Ogdon* fails both tests of *In re Oetiker*, *Ogdon* is non-analogous art. The examiner may therefore not use *Ogdon* as a reference when stating an obviousness rejection against claim 1. Accordingly, the examiner has failed to state a *prima facie* obviousness rejection of claim 1.

Nevertheless, in response to arguments, the examiners states that:

Examiner again totally disagrees with the applicant and still maintains that:

Ogdon's invention is in the field of data processing relates to a telecommunications network such as Internet, and more particularly to a network transmission, wherein such a system would allow individuals to access (*emphasis added*) and/or participate in a presentation using standard telephony and Internet network connections found in most offices and many homes (column 1, lines 47-50 of *Ogdon*). User/client cannot access, request, send, and/or receive a content without going through a standard communications network.

In response to applicant's argument that *Ogdon* is non-analogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, *Ogdon*'s field of teaching is

(Appeal Brief Page 24 of 43)
Dutta - 09/506,225

sufficient.

In addition, Ogdon does not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

Office Action of September 9, 2005, p. 13.

The examiners statements appear to be directed to the first prong of the *In re Oetiker* two-part test, whether Ogdon and the invention of claim 1 are in the same field. The examiner asserts that both Ogdon and the invention of claim 1 are in the field of data processing through a telecommunications network and, for that reason, Ogdon satisfies the first prong of the *In re Oetiker* alternative two-part test.

However, the examiner's characterization of the field of Ogdon and the claimed invention is overly-broad and insufficient to satisfy the first prong of the test in *In re Oetiker*. The "field of Applicant's endeavor" is, as shown above, identifying rewriting of universal resource locators in content requested by a user. On the other hand, Ogdon is broadly directed to providing a presentation on a network. The two fields are wholly unrelated. Thus, Ogdon fails the first test in *In re Oetiker*.

Moreover, as also quoted above, the court in *In re Oetiker* stated that "it has not been shown that a person of ordinary skill, seeking to solve a problem of fastening a hose clamp, would reasonably be expected or motivated to look to fasteners for garments." *Id.* Hose claims and fasteners for garments are both related to fasteners. Under the examiner's standards, because both hose claims and fasteners for garments are related to fasteners, the reference discussing fasteners for garments would be in the same field of endeavor as hose clamps. However, the court came to the opposite conclusion. The court in *In re Oetiker* stated that the reference discussing fasteners was unrelated to hose clamps; thus, the inquiry into whether a reference is in the same field of endeavor as the invention of claim 1 must look at what, specifically, is claimed and what, specifically, the reference teaches. The examiner's statements fail to do either because the examiner's statements are overly-broad.

In the case at hand, as shown above, Ogdon and the invention of claim 1 have wholly unrelated

(Appeal Brief Page 25 of 43)
Dutta - 09/506,223

fields of endeavor when analyzed under the specific standards of *In re Oetiker*. Thus, Ogdon fails the first test in *In re Oetiker*. The examiner does not contend that Ogdon fails the second test of *In re Oetiker* and, as shown above, Ogdon does fail the second test of *In re Oetiker*. For this reason, Ogdon is non-analogous art. Accordingly, the examiner continues to fail to state a prima facie obviousness rejection against claim 1.

The examiner's statements regarding intended use appear to be misplaced. No features in claim 1 that are at issue recite an intended use. Thus, the examiner's statements do not change the above analysis regarding *In re Oetiker*, or any other analysis discussed above.

A.1.iv The Examiner Failed to State a Prima Facie Obviousness Rejection Against Claim 1 Because Ogdon Addresses a Different Problem than that Addressed by Claim 1

Ogdon and the present invention are in different fields and address different problems. As previously shown, Ogdon is concerned with providing a presentation over a network and ensuring only authorized users access the presentation. Ogdon addresses the problem of how to make a presentation available to participants with differing network characteristics. In contrast, claim 1 addresses the problem of ensuring user privacy. The present invention detects when a content provider is monitoring user requests to access content, and prevents receipt of further content if monitoring is detected. One skilled in the art would have no motivation to modify Ogdon to address the problem of validating whether user requests to access content are being monitored. Because no motivation exists to modify Ogdon to achieve the invention of claim 1, the examiner cannot state a prima facie obviousness rejection against claim 1. The examiner failed to rebut this fact in the final office action of September 9, 2005.

A.1.v The Examiner Failed to State a Prima Facie Obviousness Rejection Against Claim 1 Because Claim 1 Solves a Problem Unrecognized by Ogdon

Claim 1 solves the problem of detecting when a content-provider is monitoring user requests to access content. Ogdon does not provide any indication that the inventor was even aware of this problem. As previously shown, in Ogdon, both the user and validation server are aware that the presentation content provider is monitoring user access to content and so there is no need to detect whether user requests are being monitored. In contrast, in the present invention, the user and validation server are unsure whether the content provider is monitoring user access to content and

so there is a need to detect when monitoring is occurring. Because claim 1 solves a problem that *Ogdon* does not recognize, no motivation exists to modify *Ogdon* to achieve the invention of claim 1. Accordingly, the examiner continues to fail to state a prima facie obviousness rejection against claim 1.

Nevertheless, in response to arguments, the examiner states that:

In response to applicant's arguments, the recitation "solves the problem of detecting" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 534 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Office Action of September 9, 2005, p. 11 (emphasis in original).

The examiner's statements are misplaced because the phrase "solves the problem of detecting" does not appear in claim 1. In addition, the examiner misunderstands Applicant's argument. Applicants are showing that no motivation exists to modify *Ogdon* to achieve the invention of claim 1. The examiner does not rebut this fact.

A.1.vi The Examiner Failed to State a Prima Facie Obviousness Rejection Against Claim 1 Because the Proposed Modification Would Result in an Unworkable Method.

The proposed modification would result in an unworkable method. The examiner does not rebut this fact.

In *Ogdon*, the validation server validates the user's presentation identifier, and if the identifier is valid, the user is allowed access to content. If the identifier is invalid, the user is not allowed access to content. *Ogdon*, column 19, lines 13-23. In contrast, in claim 1, users first access and receive content and then afterwards the validation service validates whether monitoring of user requests to access content is occurring. Furthermore, in claim 1, receipt of additional content is prevented if monitoring is detected.

If *Ogdon*'s teachings were used to modify claim 1 as suggested by the examiner, then no one would gain access to content. As users attempt to access content in the system of the proposed modification, the validation server in *Ogdon* would detect that users were accessing content. This

(Appeal Brief Page 27 of 43)
Dutta - 09/506,225

seems to be the basis for the examiner's apparent belief that monitoring of access to content inherently occurs in *Ogdon*. However, claim 1 provides that if monitoring of access to content is detected, then receipt of additional content is selectively prevented. Thus, the instant that a user attempted to gain access to content, the validation server of the proposed modification would detect the access to the content, monitor the access to the content, detect that monitoring has occurred, and, as a result, subsequently block additional receipt of content. Accordingly, the user would never receive content if the examiner's proposed modification were implemented. Permanently blocking access to content defeats the purpose of *Ogdon*, which is to provide content to users. Furthermore, permanently blocking access to content in this manner serves no useful function. Accordingly, the proposed modification would be unworkable. Therefore, no motivation exists to modify *Ogdon* to achieve the invention of claim 1. Hence, the examiner has failed to state a prima facie obviousness rejection against claim 1.

A.1.vii Remaining Claims in the Group

For the above reasons, the examiner has failed to state a prima facie obviousness rejection against claim 1. Thus, for the reasons given above, the examiner has also failed to state a prima facie obviousness rejection against the remaining claims in this group.

A.2. Claims 5 and 26

Claims 5 and 26 stand rejected under 35 U.S.C. § 103(a) as obvious over *Ogdon*. Claims 5 and 26 depend from claims discussed above. Thus, the examiner has failed to state a prima facie obviousness rejection against these claims at least for the reasons presented vis-à-vis claim 1 above. In addition, the examiner has failed to state a prima facie obviousness rejection with respect to these claims because *Ogdon* does not teach what the examiner asserts vis-à-vis these claims.

Claim 5 is a representative claim in this grouping of claims. Claim 5 is as follows:

5. The method of claim 1, wherein the step of selectively preventing receipt of content from the source comprises:
 - presenting an indication of monitoring of user requests to access the received content is occurring by the source; and
 - responsive to receiving user input indicating that receipt of additional content from the source should be prevented, preventing receipt of the additional content from the source.

Ogdon does not teach the claimed feature of "presenting an indication of monitoring of user requests to access the received content is occurring by the source." As discussed above, Ogdon is unconcerned with determining whether user requests are being monitored. Instead, Ogdon teaches a system for allowing presentation givers and audience members to have access to a single presentation environment over a network.

The examiner ignores these features. The examiner states that "these claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above." However, the claim 5 is patentably distinct from claim 1 because Ogdon does not show the additional features of claim 5. Furthermore, Ogdon provides no indication that an indication of monitoring should be presented to anyone. Thus, Ogdon does not teach or suggest all of the features of claim 5.

Because Ogdon does not teach or suggest the features of claim 5, the examiner has failed to state a *prima facie* obviousness rejection against claim 5. In addition, because the examiner has not stated a motivation to further modify Ogdon to achieve the invention of claim 5, the examiner has again failed to state a *prima facie* obviousness rejection against claim 5. For similar reasons, the examiner has also failed to state a *prima facie* obviousness rejection against claim 26.

A.3. Claims 6 and 27

Claims 6 and 27 stand rejected under 35 U.S.C. § 103(a) as obvious over *Ogdon*. Claims 6 and 27 depend from claims discussed above. Thus, the examiner has failed to state a *prima facie* obviousness rejection against claim these claims at least for the reasons presented vis-à-vis claim 1 above. In addition, the examiner has failed to state a *prima facie* obviousness rejection with respect to these claims because Ogdon does not teach what the examiner asserts vis-à-vis these claims.

Claim 6 is a representative claim in this grouping of claims. Claim 6 is as follows:

6. The method of claim 5, wherein the step of preventing receipt of content from the source comprises:
including an identification of the source in a service used to prevent receipt of content from identified sources.

Ogdon does not teach the claimed feature of "including an identification of the source in a service used to prevent receipt of content from identified sources." As discussed above, Ogdon is unconcerned with determining whether user requests are being monitored. Instead, Ogdon teaches

a system for allowing presentation givers and audience members to have access to a single presentation environment over a network.

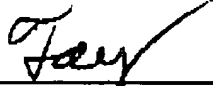
The examiner ignores these features. The examiner states that "these claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above." However, the claim 6 is patentably distinct from claim 1 because Ogdon does not show the additional features of claim 6. Furthermore, Ogdon provides no indication that the source from which receipt of content is prevented should be identified. Thus, Ogdon does not teach or suggest all of the features of claim 6.

Because Ogdon does not teach or suggest the features of claim 6, the examiner has failed to state a prima facie obviousness rejection against claim 6. . In addition, because the examiner has not stated a motivation to further modify Ogdon to achieve the invention of claim 6, the examiner has again failed to state a prima facie obviousness rejection against claim 6. For similar reasons, the examiner has also failed to state a prima facie obviousness rejection against claim 27.

B. CONCLUSION

The examiner has failed to state a prima facie obviousness rejection against any of the claims because (i) features that the examiner states as being present in *Ogdon* are not taught or suggested in *Ogdon*, (ii) the examiner has failed to state a proper motivation to modify the reference, (iii) *Ogdon* is non-analogous art, (iv) *Ogdon* addresses a different problem than that addressed by claim 1, (v) claim 1 solves a problem unrecognized by *Ogdon*, and (vi) because the proposed modification would result in an unworkable method. In addition, the examiner has also failed to state a prima facie obviousness rejection against claims 5 and 26 and 6 and 27 for the additional reasons provided above.

For the above reasons, Applicants request that the Board of Patent Appeals and Interferences overturn the rejections and allow the claims.



Theodore D. Fay III
Reg. No. 48,504
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

(Appeal Brief Page 30 of 43)
Dutta - 09/506,225

CLAIMS APPENDIX

The text of the claims involved in the appeal is:

1. A method in a data processing system for detecting monitoring of access to content, the method comprising the data processing system implemented steps of:
 - requesting the content from a source using a set of identifiers;
 - receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content;
 - sending identifiers to a validation service, wherein the ~~set of~~ identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the content at the source; and
 - responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, selectively preventing receipt of additional content from the source.
2. The method of claim 1, wherein the source is a Web server.
3. The method of claim 1, wherein the content is a Web page.
4. The method of claim 1, wherein the validation service is located on a server.
5. The method of claim 1, wherein the step of selectively preventing receipt of content from the source comprises:

(Appeal Brief Page 31 of 43)
Dutta - 09/506,225

presenting an indication of monitoring of user requests to access the received content is occurring by the source; and

responsive to receiving user input indicating that receipt of additional content from the source should be prevented, preventing receipt of the additional content from the source.

6. The method of claim 5, wherein the step of preventing receipt of content from the source comprises:

including an identification of the source in a service used to prevent receipt of content from identified sources.

7. The method of claim 1, wherein the identifier is a universal resource locator.

8. A method in a data processing system for detecting monitoring of access to content, the method comprising the data processing system implemented steps of:

receiving a request from a requestor to determine whether a source of the content is monitoring access by the requestor, wherein the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to the first number of identifiers;

sending a new request to the source using an identifier from the first number of identifiers in the set of identifiers;

receiving a first response from the source, wherein the response includes a return identifier;

comparing the set of identifiers to the return identifier; and

generating a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers.

9. The method of claim 8 further comprising sending the second response to the requestor.
10. The method of claim 8, wherein the source is a Web server.
11. The method of claim 8, wherein the content is a Web page, wherein the first number of identifiers is a first universal resource locator sent by the requestor for the Web page, and wherein the second number of identifiers is a second universal resource locator that identifies a location of the Web page returned from the source in response to the requestor sending the first universal resource locator to the source.
12. The method of claim 8, wherein the return identifier is a universal resource locator.
13. The method of claim 8, wherein the set of identifiers are in an order used to reach the selected content and wherein the sending, receiving, and comparing steps are performed for each of the identifiers within the set of identifiers.

14. The method of claim 8, wherein the step of generating the response comprises:
placing an identification of the source in the response.
15. The method of claim 8, wherein an identification of the source is a domain name for the source.
16. A browser program for use in a data processing system, the browser program comprising:
a communications interface, wherein the communications interface receives content from a network;
a graphical user interface used to display the content;
a language interpretation unit, wherein the language interpretation unit processes content received by the communications interface for display on the graphical user interface; and
a detection unit, wherein the detection unit requests the content from a source using a set of identifiers; receives the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the contents at the source; sends identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the received content; and selectively prevents receipt of additional content from the source in response to receiving a response from the validation service indicating the monitoring of user requests to access to received content is occurring.

17. The browser program of claim 16, wherein the language interpretation unit interprets hypertext markup language statements.

18. The browser program of claim 16, wherein the language interpretation unit interprets JavaScript.

19. A data processing system comprising:

a bus;

a communications interface connected to the bus, wherein the communications interface is configured for connection to a network;

a processing unit connected to the bus, wherein the processing unit executes instructions; and

a memory connected to the bus, wherein the memory includes instructions used to request the content from a source using a set of identifiers; receive the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the received contents at the source; send a identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the received content; and selectively prevent receipt of additional content from the source in response to receiving a response from the validation service indicating monitoring of user requests to access to the received content is occurring.

20. The data processing system of claim 19, wherein the communications interface is one of a network adapter and a modem.

21. A data processing system comprising:

a bus;

a communications interface connected to the bus, wherein the communications interface is configured for connection to a network;

a processing unit connected to the bus, wherein the processing unit executes instructions;

and

a memory connected to the bus, wherein the memory includes instructions used to receive a request from a requestor to determine whether a source of the content is monitoring access by the requestor in which the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to the first number of identifiers; send a new request to the source using an identifier from the first number of identifiers in the set of identifiers, receive a first response from the source in which the response includes a return identifier, compare the set of identifiers to the return identifier, and generate a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers.

22. A data processing system for detecting monitoring of access to content, the data processing system comprising:

requesting means for requesting the content from a source using a set of identifiers;

receiving means for receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content at the source;

sending means for sending identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the received content; and

preventing means responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, for selectively preventing receipt of additional content from the source.

23. The data processing system of claim 22, wherein the source is a Web server.

24. The data processing system of claim 22, wherein the content is a Web page.

25. The data processing system of claim 22, wherein the validation service is located on a server.

26. The data processing system of claim 22, wherein the preventing means comprises:

presenting means for presenting an indication of monitoring of user requests to access the content is occurring by the source; and

means responsive to receiving user input indicating that receipt of the additional content from the source should be prevented, for preventing receipt of additional content from the source.

27. The data processing system of claim 26, wherein the preventing means comprises:
including means for including an identification of the source in a service used to prevent receipt of content from identified sources.

28. The data processing system of claim 22, wherein the identifier is a universal resource locator.

29. A data processing system for detecting monitoring of access to content, the data processing system comprising:

first receiving means for receiving a request from a requestor to determine whether a source of the content is monitoring access by the requestor, wherein the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to the first number of identifiers;

sending means for sending a new request to the source using an identifier from the first number of identifiers in the set of identifiers;

second receiving means for receiving a first response from the source, wherein the response includes a return identifier;

comparing means for comparing the set of identifiers to the return identifier; and

generating means for generating a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers.

30. The data processing system of claim 29 further comprising sending the response to the requestor.

31. The data processing system of claim 29, wherein the source is a Web server.

32. The data processing system of claim 29, wherein the content is a Web page, wherein the first number of identifiers is a first universal resource locator sent by the requestor for the Web page, and wherein the second number of identifiers is a second universal resource locator that identifies a location of the Web page returned from the source in response to the requestor sending the first universal resource locator to the source.

33. The data processing system of claim 29, wherein the identifier is a universal resource locator.

34. The data processing system of claim 29, wherein the set of identifiers are in an order used to reach the selected content and wherein the sending, receiving, and comparing steps are performed for each of the identifiers within the set of identifiers.

35. The data processing system of claim 29, wherein the generating means comprises:

placing means for placing an identification of the source in the response.

36. The data processing system of claim 29, wherein an identification of the source is a domain name for the source.

37. A computer program product in a computer readable medium for detecting monitoring of access to content, the computer program product comprising:

first instructions for requesting the content from a source using a set of identifiers;

second instructions for receiving the content from the source to form received content,

wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content at the source;

third instructions for sending identifiers used to reach the received content to a validation service, wherein the identifiers include each identifier used to request the received content and each returned identifier representing the location of the received content; and

fourth instructions, responsive to a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, for selectively preventing receipt of additional content from the source.

38. A computer program product in a computer readable medium for detecting monitoring of access to content, the computer program product comprising:

first instructions for receiving a request from a requestor to determine whether a source of the content is monitoring access by the requestor, wherein the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of

identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a location of the content at the source returned to the requestor in response to the first number of identifiers;

second instructions for sending a new request to the source using an identifier from the first number of identifiers in the set of identifiers;

third instructions for receiving a first response from the source, wherein the response includes a return identifier;

fourth instructions for comparing the set of identifiers to the return identifier; and

fifth instructions for generating a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers.

39. The method of claim 8, wherein the content is a plurality of Web pages, wherein the first number of identifiers contain first universal resource locators sent by the requestor for the plurality of Web pages, and wherein the second number of identifiers contain second universal resource locators that identify the plurality of Web pages returned from the source in response to the requestor sending the first universal resource locators to the source.

EVIDENCE APPENDIX

There is no additional evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.

returned identifier to a validation service, or (c) responsive to the validation service indicating monitoring of user requests to access content is occurring, selectively preventing receipt of additional content from the source.

The examiner asserts that *Ogdon* does show these features, citing *Ogdon* as discussed in the previous response to office action. However, contrary to the examiner's assertions, *Ogdon* does not teach or suggest receiving content *and* at least one returned identifier. In claim 1, the returned identifier is not part of the set of identifiers used to access the content. *Ogdon* teaches using an audience member identifier to initially access presentation content. *Ogdon* does not teach or suggest receiving at least one returned identifier in addition to receiving content. Thus, *Ogdon* does not teach or suggest all of the features as suggested by the examiner.

Regarding the feature of sending the set of identifiers used to request the received content and each returned identifier to a validation service, *Ogdon* does not teach or suggest sending the set of identifiers used to request the received content *and* each returned identifier to a validation service because *Ogdon* makes no mention of a returned identifier. *Ogdon* teaches providing registered clients a presentation identifier and validating the presentation identifier before allowing clients access. *Ogdon* does not teach or suggest sending the identifiers used to request content and each returned identifier to a validation service after receiving content. Thus, *Ogdon* does not teach or suggest all of the features of claim 1.

Regarding the feature of validation, *Ogdon* uses a validation server and the present invention uses a validation service. Merely because both *Ogdon* and claim 1 use the word 'validation' does not mean that both are the same. The validation service in claim 1 is provided with different parameters, has a different purpose, and is used in a different context than *Ogdon*'s validation server, as described in detail below.

In *Ogdon*, the content provider validates the audience member's identifier before allowing the audience member access to content. In contrast, in the present invention, the user accesses a content provider and receives content, and then a validation service is used to detect whether the content provider is monitoring user requests to access content.

In *Ogdon*, validation is described as follows:

In step 416, the pre-show control system 136 accepts network 70 and/or network 74 connections by candidate clients for the presentation performance. Note that it is assumed that the clients have previously registered for the presentation performance with the registration module 140